Empfehlungen zur Passwortgestaltung

Leitfaden

Stand: April 2024

Postanschrift
Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Mecklenburg-Vorpommern

Lennéstraße 1
19053 Schwerin

Hausanschrift
Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Mecklenburg-Vorpommern

Werderstraße 74a
19055 Schwerin

Kommunikation
Telefon (03 85) 5 94 94-0

E-Mail info@datenschutz-mv.de
Internet www.datenschutz-mv.de

Der Landesbeauftragte für
DATENSCHUTZ und
INFORMATIONSFREIHEIT
Mecklenburg-Vorpommern

Einleitung

Ein Passwort dient dem Schutz persönlicher Daten und sensiblen Informationen. Wenn beispielsweise Kriminelle Zugriff auf Daten erlangen, können sie mit einer Kontoübernahme oder Identitätsdiebstahl den Betroffenen materiellen und persönlichen Schaden zufügen. Darum ist es unerlässlich, ein sicheres Passwort festzulegen. Es ist ratsam, nach Möglichkeit die Zwei-Faktor-Authentifizierung (2FA) zu aktivieren sofern diese vom jeweiligen Dienst angeboten wird, um eine zusätzliche Sicherheitsebene für das Konto einzurichten.

Zweck und Anforderungen

Der Zweck dieses Leitfadens besteht darin, Benutzenden die notwendigen Informationen bereitzustellen, um starke und sichere Passwörter zu erstellen, zu verwenden und zu verwalten. Die Anforderungen zielen darauf ab, die Vertraulichkeit und Integrität von Informationen und persönlichen Daten zu schützen und das Risiko von Sicherheitsverletzungen zu minimieren.

Grundsätze

In Anlehnung an die Vorgaben des BSI sollten beim Handling mit Passwörtern folgende Aspekte beachtet werden:

- Das Passwort sollte mindestens 16 Zeichen lang sein und aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen.
- Ein WLAN-Passwort bzw. Netzwerkschlüssel muss besonders lang und komplex gestaltet sein. Das WLAN-Passwort ist nicht identisch mit dem Router-Passwort. Es dient speziell dem drahtlosen Zugang in das lokale Funknetz. Das voreingestellte Passwort des Herstellers sollte immer geändert werden und mindestens 20 Zeichen lang sein und aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen.
- Ein Passwort sollte nicht Begriffe mit Bezug zum Passworterstellen enthalten und nicht aus einfachen Zeichenfolgen (wie 123456) oder Wörterbuchbegriffe basieren.
- Initial-, Startpasswörter bzw. voreingestellte Passwörter (z. B. des Herstellers bei Auslieferung von Systemen – sog. Default-Passwörter) sind immer durch individuelle Passwörter zu ersetzen.

- Für jedes Konto ein einzigartiges Passwort zu verwenden, um das Risiko von Kompromittierungen zu verringern.

- Das Passwort sollte nur dem Benutzenden bekannt sein und immer geheim gehalten werden.

- Passwörter sollten nicht auf programmierbaren Funktionstasten gespeichert werden.

- Passwörter müssen immer vor unberechtigten Zugriffen geschützt und sollten nicht in sichtbaren oder in unmittelbaren Nutzungsbereichen hinterlegt werden.

- Bei der Eingabe sollte das Passwort nicht auf dem Bildschirm angezeigt werden.

- Bei Verdacht auf Kenntnisnahme des Passworts durch unbefugte Dritte oder Malwarebefall ist das Passwort unverzüglich zu wechseln.

- Alte Passwörter sollten nach einem Passwortwechsel nicht mehr verwendet werden.

- Grundsätzlich sollte der Passwortschutz mit einem zusätzlichen Faktor (2FA bzw. MFA) erfolgen. Das kann auf bspw. Basis von Biometrie (bspw. Fingerabdruck), Token oder TAN-Verfahren umgesetzt werden.

- Zunehmend erfolgt auch bei einigen Diensteanbietern die Nutzung von Passkeys als sicherere Alternative zum Passwort.

Dienstliche Passwortnutzung:

- Im Arbeitsumfeld sollten Richtlinien für die gesamte Institution für eine ausreichende und einheitliche Sicherheit sorgen.

- Für besonders privilegierte Konten bzw. Rollen (bspw. Systemadministratoren) sollten geteilte Passworte verwendet werden, die von zwei Personen einzugeben sind („Vier-Augen-Prinzip“).

- Die Benutzerkonten von Mitarbeitenden der Administration müssen immer getrennt werden nach Konten für normale Arbeitsaufgaben und Konten mit weitreichenden Berechtigungen (Administration).

- Passwörter für Konten mit weiterreichenden Rechten sollten mind. 20 Zeichen lang sein.

- Die Sicherheitseinstellungen für Passwörter (bspw. Länge) sollten durch technische Maßnahmen erzwungen werden.

- Die Wiederholung alter Passwörter beim Passwortwechsel sollte vom IT-System verhindert werden (Passwort-Historie).

- Nach spätestens 5-maligen Fehlversuchen bei der Passworteingabe sollte das Benutzerkonto gesperrt werden. Fehlversuche bei der Passworteingabe und die Sperrung von Benutzerkonten müssen protokolliert werden.

- Bei der Authentisierung in vernetzten Systemen sollten Passwörter nur verschlüsselt übertragen werden.

- Die Passwörter sollten im System zugriffssicher gespeichert werden, zum Beispiel mittels Einwegverschlüsselung.

Möglichkeiten im Umgang von Passwörtern

Zur sicheren und unterstützenden Verwaltung von Passwörtern ist es ratsam, Passwortmanager einzusetzen. Es gibt verschiedene Apps, die auch auf Mobilgeräten nutzbar sind. Mit ihnen lassen sich zudem sichere Passwörter zufällig generieren bzw. das selbsterstellte Passwort auf Stärke überprüfen. Hier ist es wichtig, dass das Passwort des Passwortmanagers (Master-Passwort) besonders sicher gestaltet ist, da er quasi der Schlüssel für den Passwort-Tresor darstellt. Zudem sollte immer ein Backup der Passwortdatenbank erfolgen.

Es lassen sich merkbare geforderte komplexe Passwörter wie im Folgenden beschrieben selber erstellen. Man denkt sich einen Satz aus und benutzt von jedem Wort nur den ersten Buchstaben (oder nur den dritten oder letzten etc.).
Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen.

<u>Beispiel:</u>

Morgens **s**tehe **i**ch **u**m **6** **U**hr **a**uf **u**nd **m**ache **m**ir **e**rst **m**al **g**anz **g**emütlich **e**inen **K**affee.

1. Schritt: Anfangsbuchstaben/Zahlen
   Msiu6Uaummemggek
2. Schritt: Sonderzeichen: aus s = $ / aus u(nd) = &
   M$iu6Ua&mmemggeK

Der Landesbeauftragte für
DATENSCHUTZ und
INFORMATIONSFREIHEIT
Mecklenburg-Vorpommern

Weiterführende Hinweise

https://www.deutschland.de/de/topic/politik/deutschland-cybersicherheit-bsi-passwort-und-sicherheit

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html

https://www.heise.de/download/specials/Passwort-Manager-Tipps-Tools-fuer-die-Passwort-Verwaltung-6033009

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Sicherheitstipps-fuer-privates-und-oeffentliches-WLAN/sicherheitstipps-fuer-privates-und-oeffentliches-wlan_node.html